Billing Code: 5001-06

DEPARTMENT OF DEFENSE

Office of the Secretary

32 CFR Part 310

[Docket ID: DOD-2019-OS-0122]

RIN 0790–AK47

Privacy Act of 1974; Implementation

AGENCY: Office of the Secretary of Defense, DoD.

ACTION: Direct final rule with request for comments.

SUMMARY: The Office of the Secretary proposes to exempt records maintained in CIG-26, "Case Control System–Investigative." The System of Records Notice was published in the Federal Register on August 9, 2011. This rule is being published as a direct final rule as the DoD does not expect to receive any adverse comments. If such comments are received, this direct final rule will be cancelled and a proposed rule for comments will be published.

DATES: The rule will be effective on [INSERT DATE 70 DAYS FROM PUBLICATION IN FEDERAL REGISTER] unless comments are received that would result in a contrary determination. Comments will be accepted on or before [INSERT DATE 60 DAYS FROM PUBLICATION IN FEDERAL REGISTER].

ADDRESSES: You may submit comments, identified by docket number and title, by any of the following methods.

* Federal eRulemaking Portal: http://www.regulations.gov.

Follow the instructions for submitting comments.

* Mail: DoD cannot receive written comments at this time due to the COVID-19 pandemic. Comments should be sent electronically to the docket listed above.

Instructions: All submissions received must include the agency name and docket number or Regulatory Information Number (RIN) for this Federal Register document. The general policy for comments and other submissions from members of the public is to make these submissions available for public viewing on the Internet at http://www.regulations.gov as they are received without change, including any personal identifiers or contact information.

FOR FURTHER INFORMATION CONTACT: Ms. Anna Rivera, 703-699-5680.

SUPPLEMENTARY INFORMATION: The Office of the Secretary proposes to exempt records maintained in CIG-26, "Case Control System–Investigative," from subsections (c)(3) and (c)(4); (d); (e)(1), (e)(2), (e)(3), (e)(4)(G), (e)(4)(H), (e)(4)(I), (e)(5), and (e)(8); and (g) of the Privacy Act pursuant to 5 U.S.C. 552a (j)(2), (k)(1), and (k)(2).

This direct final rule adds to the Office of the Inspector General (OIG) exemptions found in 32 CFR 310.28. This exemption rule will allow the DoD OIG to efficiently and effectively implement the DoD Inspector General program by exempting certain records from pertinent provisions of 5 U.S.C. 552a.

The DoD OIG maintains this system of records in order to carry out its responsibilities pursuant to the Inspector General Act of 1978, as amended. The DoD OIG is statutorily directed to conduct and supervise investigations relating to the programs and operations of the DoD; to promote economy, efficiency, and effectiveness in the administration of such programs and operations; and to prevent and detect fraud, waste, and abuse in such programs and operations. Accordingly, the records in this system are used in the course of investigating individuals suspected of administrative or criminal misconduct.

Executive Order 12866, "Regulatory Planning and Review" and Executive Order 13563, "Improving Regulation and Regulatory Review"

It has been previously determined that all Privacy Act rules for the Department of Defense are not significant rules. The rules do not: (1) Have an annual effect on the economy of $100 million or more or adversely affect in a material way the economy; a sector of the economy; productivity; competition; jobs; the environment; public health or safety; or State, local, or tribal governments or communities; (2) Create a serious inconsistency or otherwise interfere with an action taken or planned by another Agency; (3) Materially alter the budgetary impact of entitlements, grants, user fees, or loan programs, or the rights and obligations of recipients thereof; or (4) Raise novel legal or policy issues arising out of legal mandates, the President's priorities, or the principles set forth in these Executive Orders.

Executive Order 13771, "Reducing Regulation and Controlling Regulatory Costs"

This final rule is not subject to the requirements of E.O. 13771 because it is not significant under E.O. 12866.

Section 202, Public Law 104-4, "Unfunded Mandates Reform Act"

It has been determined that the Privacy Act rulemaking for the Department of Defense does not involve a Federal mandate that may result in the expenditure by State, local and tribal governments, in the aggregate, or by the private sector, of $100 million or more and that such rulemaking will not significantly or uniquely affect small governments.

Public Law 96-511, "Paperwork Reduction Act" (44 U.S.C. Chapter 35)

It has been determined that Privacy Act rules for the Department of Defense impose no additional reporting or recordkeeping requirements on the public under the Paperwork Reduction Act of 1995.

Public Law 96-354, "Regulatory Flexibility Act" (5 U.S.C. Chapter 6)

It has been certified that Privacy Act rules for the Department of Defense do not have significant economic impact on a substantial number of small entities because they are concerned only with the administration of Privacy Act systems of records within the Department of Defense.

Congressional Review Act

The Congressional Review Act, 5 U.S.C. 801 et seq., generally provides that before a rule may take effect, the agency promulgating the rule must submit a rule report, which includes a copy of the rule, to each House of the Congress and to the Comptroller General of the United States. We will submit a report containing this rule and other required information to the U.S. Senate, the U.S. House of Representatives, and the Comptroller General of the United States. A major rule cannot take effect until 60 days after it is published in the Federal Register. This direct final rule is not a "major rule" as defined by 5 U.S.C. 804(2).

Executive Order 13132, "Federalism"

It has been determined that the Privacy Act rules for the Department of Defense do not have federalism implications. The rules do not have substantial direct effects on the States, on the relationship between the National Government and the States, or on the distribution of power and responsibilities among the various levels of government.

List of Subjects in 32 CFR Part 310

Privacy.

Accordingly, 32 CFR part 310 is amended as follows:

PART 310—[AMENDED]

1. The authority citation for part 310 continues to read as follows:

Authority: 5 U.S.C. 552a.

2. Amend § 310.28 by adding paragraph (c)(9) to read as follows:

§ 310.28 Office of the Inspector General (OIG) exemptions.

* * * * *

(c) * * *

(9) *System identifier and name.* CIG-26, Case Control System–Investigative.

(i) *Exemption.* Any portion of this system which falls within the provisions of 5 U.S.C. 552a(j)(2) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (c)(4), (d), (e)(1), (e)(2), (e)(3), (e)(4)(G) through (I), (e)(5), (e)(8), and (g), as applicable. In addition, any portion of this system which falls within the provisions of 5 U.S.C. 552a(k)(1) or (k)(2) may be exempt from the following subsections of 5 U.S.C. 552a: (c)(3), (d), (e)(1), (e)(4)(G) through (I), as applicable. Exempted records from other systems of records may in-turn become part of the case record in this system. To the extent that copies of exempt records from those 'other' systems of records are entered into this system, the DoD OIG claims the same exemptions for the records from those 'other' systems that are entered into this system, as claimed for the original primary system of which they are a part. Records are only exempt from pertinent provisions of 5 U.S.C. 552a to the extent such provisions have been identified and an exemption claimed for the original record and the purposes underlying the exemption for the original record still pertain to the record which is now contained in this system of records. The exemption rule for the original records will identify the specific reasons why the records are exempt from specific provisions of 5 U.S.C. 552a.

(ii) *Authority.* 5 U.S.C. 552a(j)(2), (k)(1), and (k)(2).

(iii) *Reasons.* (A) From subsections (c)(3) and (c)(4) because making available to a record subject the accounting of disclosure of investigations concerning him or her would specifically reveal an investigative interest in the individual. Revealing this information would reasonably be expected to compromise open or closed administrative or criminal investigation efforts to a known or suspected offender by notifying the record subject that he or she is under investigation. This information could also prompt the record subject to take measures to impede the investigation, e.g. destroy evidence, intimidate potential witnesses, or flee the area to avoid or impede the investigation.

(B) From subsection (d), because these provisions concern individual access to and amendment of certain records contained in this system. Granting access to information that is properly classified pursuant to executive order may cause damage to national security. Additionally, compliance with these provisions could alert the subject of an investigation of the fact and nature of the investigation and/or the investigative interest of law enforcement agencies. It can also compromise sensitive information related to national security; interfere with the overall law enforcement process by leading to the destruction of evidence, improper influencing of witnesses, fabrication of testimony, and/or flight of the subject; could identify a confidential source or disclose information which would constitute an unwarranted invasion of another's personal privacy; reveal a sensitive investigation or constitute a potential danger to the health or safety of law enforcement personnel, confidential informants, and witnesses. Amendment of open or active investigations would interfere with ongoing law enforcement investigations and analysis activities, and impose an excessive administrative burden by requiring investigations, analyses, and reports to be continuously reinvestigated and revised.

(C) From subsection (e)(1) because it is not always possible to determine what information is relevant and necessary at an early stage in a given investigation, and because DoD OIG and other agencies may not always know what information about a known or suspected offender may be relevant to law enforcement for the purpose of conducting an operational response. The nature of the criminal and/or administrative law enforcement investigative functions creates unique problems in prescribing a specific parameter and a particular case with respect to what information is relevant or necessary. Also, due to the DoD OIG's close liaison and working relationships with other Federal, State, local and foreign country criminal and administrative law enforcement agencies, information may be received which may relate to a case under the investigative jurisdiction of another agency. The maintenance of this information may be necessary to provide leads for appropriate criminal and administrative law enforcement purposes and to establish patterns of activity which may relate to the jurisdiction of other cooperating agencies.

(D) From subsection (e)(2) because it is not always in the best interest of law enforcement to collect information to the greatest extent practicable directly from an investigative subject. Requiring the collection of information to the greatest extent practicable directly from an investigative subject would present a serious impediment to law enforcement in that the subject of the investigation would be placed on notice of the existence of the investigation and would therefore be able to avoid detection.

(E) From subsection (e)(3) because supplying an individual with a form containing a Privacy Act Statement would tend to inhibit cooperation by many individuals involved in a

criminal investigation. The effect would be somewhat adverse to established investigative methods and techniques.

(F) From subsections (e)(4)(G) through (I) because this system of records is exempt from the access provisions of subsection (d).

(G) From subsection (e)(5) because the requirement that records be maintained with attention to accuracy, relevance, timeliness, and completeness would unfairly hamper the investigative process. It is the nature of criminal law enforcement for investigations to uncover the commission of illegal acts at diverse stages. It is frequently impossible to determine initially what information is accurate, relevant, timely, and complete. With the passage of time, seemingly irrelevant or untimely information may acquire new significance as further investigation brings new details to light.

(H) From subsection (e)(8) because the notice requirements of this provision could present a serious impediment to criminal law enforcement investigations by revealing investigative techniques, procedures, and existence of sensitive information and/or confidential sources.

(I) To the extent that exemptions have been established from other provisions of the Privacy Act, the civil remedies provisions of subsection (g) are inapplicable. The nature of criminal law enforcement investigations and the utilization of authorized exemptions should not increase the Department's exposure to civil litigation under the Privacy Act.

Dated: September 23, 2020.

Aaron T. Siegel,

Alternate OSD Federal Register Liaison Officer, Department of Defense.

[FR Doc. 2020-21379 Filed: 9/25/2020 8:45 am; Publication Date: 9/28/2020]